Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 26 janvier 2007
N° CERTA-2007-AVI-057

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur Hitachi Web Server

Gestion du document

Référence	CERTA-2007-AVI-057
Titre	Vulnérabilités sur Hitachi Web Server
Date de la première version	26 janvier 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Hitachi HS06-022 du 24 janvier 2007
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Contournement de la politique de sécurité ;
- attaque de type *cross-site scripting*.

2 Systèmes affectés

- Hitachi Web Server ;
- Hitachi Web Server Security Enhancement ;
- Hitachi Web Server Custom Edition ;
- Hitachi Web Server for VOS3 ;
- Hitachi uCosminexus Service Platform ;
- Hitachi uCosminexus Service Architect ;
- Hitachi uCosminexus Developer Standard ;
- Hitachi uCosminexus Developer Professional ;
- Hitachi uCosminexus Developer Light ;
- Hitachi uCosminexus Application Server Standard ;
- Hitachi uCosminexus Application Server Smart Edition ;
- Hitachi uCosminexus Application Server Enterprise ;

- Hitachi Cosminexus Server Web Edition 0 et 4 ;
- Hitachi Cosminexus Standard Edition 0 et 4 ;
- Hitachi Cosminexus Enterprise Edition ;
- Hitachi Cosminexus Developer Standard 6 ;
- Hitachi Cosminexus Developer Professional 6 ;
- Hitachi Cosminexus Developer 5 ;
- Hitachi Cosminexus Application Server Standard 6 ;
- Hitachi Cosminexus Application Server Enterprise 6 ;
- Hitachi Cosminexus Application Server 5.

3 Résumé

Trois vulnérabilités sur *Hitachi Web Server* permettraient à une personne malintionnée d'exécuter une attaque de type *cross-site scripting* et/ou un contournement de la politique de sécurité.

4 Description

Trois vulnérabilités sont présentes sur *Hitachi Web Server*. La première concerne une vulnérabilité dans *OpenSSL* permettant de forcer le serveur à utiliser *SSL 2.0* au lieu de *SSL 3.0*. Les deux autres vulnérabilités sont de type *cross-site scripting*. Pour plus d'informations, vous pouvez consulter les avis CERTA-2005-AVI-400 et CERTA-2005-AVI-490.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Hitachi du 24 janvier 2007 :
  http://www.hitachi-support.com/security_e/vuls_e/HS06-022_e/01-e.html
- Référence CVE CVE-2005-3352 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3352
- Référence CVE CVE-2005-2969 :
  http://cve.mitre.org/cg-bin/cvename.cgi?name=CVE-2005-2969
- Avis du CERTA du 12 octobre 2005 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-400/CERTA-2005-AVI-400.html
- Avis du CERTA du 15 décembre 2005 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-490/CERTA-2005-AVI-490.html

Gestion détaillée du document

26 janvier 2007 version initiale.